

REMARKS

The Examiner has revised the current rejection in light of new prior art and has reformulated the rejection. As set forth below, such new rejection is still deficient. However, despite such deficiencies and in the spirit of expediting the prosecution of the present application, applicant has amended each of the independent claims. Since the subject matter of such amendments was already considered by the Examiner, it is asserted that such claim amendments would not require new search and/or consideration.

The Examiner has rejected Claims 1, 16-17, 32-33 and 48-81 under 35 U.S.C. 103(a) as being unpatentable over Ackroyd (U.S. Patent Application No. 2003/0131256), in view of Hansen et al. (U.S. Patent No. 6,493,755). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to each of the independent claims.

With respect to each of the independent claims, the Examiner has relied on paragraphs [0011-0014] and [0030-0032] in Ackroyd to make a prior art showing of applicant's claimed technique "wherein the level of the detected malware event comprises one of: informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected." Specifically, the Examiner has argued Ackroyd teaches that, "for example, a particular preferred anti-malware action [that] may be triggered is to force an update of malware definition data being used; to deal with the malware by disinfecting, repairing or deleting the infected files or emails as appropriate and possibly isolating one or more portions of the computer network from the rest of the computer network in order to isolate a malware outbreak."

Applicant respectfully asserts that although Ackroyd discloses anti-malware actions (paragraph [0013-0014]), Ackroyd does not disclose that such actions are

associated with any sort of “level of the detected malware event,” in the context claimed by applicant. Specifically, Ackroyd does not teach “informational malware events...warning malware events...minor malware events...,” etc., let alone where each level of malware event has an associated action, as claimed by applicant.

Still with respect to each of the independent claims, the Examiner has again relied on paragraphs [0011-0014] and [0030-0032] in Ackroyd for substantially the same reasons cited above, to make a prior art showing of applicant’s claimed technique “wherein the level of the event trigger threshold comprises one of: informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected.” As argued above, applicant respectfully asserts that simply nowhere in Ackroyd is there any disclosure of a level, in the context claimed by applicant.

Further, with respect to each of the independent claims, the Examiner has relied on Col. 1, line 40-Col. 2, line 44 and Col. 4, lines 20-38 in Hansen to make a prior art showing of applicant’s claimed technique “wherein the transmitting step comprises the steps of: transmitting the notification of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold; and transmitting the notification of the detected malware event eventually, if the level of the detected malware event is less than the event trigger threshold; wherein the event trigger threshold is configurable to control an amount of the notifications that are received in real-time.”

The Examiner has specifically argued that Hansen teaches “automatically defining conditions under which a user/administrator is notified of network activity” and that “these notification actions could be implemented in real-time or eventually.” The Examiner has further argued that Hansen teaches that “a corresponding alarm severity class/level can be set to limit triggering of the notification rules based on...the threshold.”

After careful review of the excerpts relied on by the Examiner, applicant notes that the notification rules disclosed in Hansen only relate to thresholds of “a number of dropped or lost data packets” (see Col. 1, lines 54-55; and Col. 2, lines 63-65). Thus, the alarm threshold conditions and the alarm severity classes are only based on a threshold of a number of dropped packets. Clearly, such threshold in Hansen does not meet applicant’s claimed “level of the detected malware event” (emphasis added).

Furthermore, simply because the notifications in Hansen could be implemented in real-time or eventually (which applicant notes is not specifically disclosed in Hansen), Hansen does not meet applicant’s specific claim language as to when such notifications are transmitted in real-time and eventually, namely “transmitting the notification of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold; and transmitting the notification of the detected malware event eventually, if the level of the detected malware event is less than the event trigger threshold” (emphasis added), as claimed.

Still yet, applicant respectfully asserts that, contrary to the Examiner’s contention, the feature where “a corresponding alarm severity class/level can be set to limit triggering of the notification rule based on the extent to which the threshold has been exceeded” is not taught in Hansen. In particular, Hansen discloses different types of alarm events for different thresholds such that a specific type of alarm event is triggered based on the extent to which a threshold has been exceeded. Thus, in Hansen, an alarm event is triggered any time a packet is dropped, and only the type of alarm event (e.g. cleared, indeterminate, minor, major, and critical) is based on the threshold exceeded. Furthermore, Hansen even teaches “an ‘informational’ alarm severity class...to provide information for devices not exceeding normal operating conditions” (Col. 1, line 67-Col. 2, line 2-emphasis added). In this way, alarm events are triggered even when a threshold has not been met, which clearly would not “limit triggering of the notification rule,” as argued by the Examiner.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant thus respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Nevertheless, despite the foregoing paramount distinctions and in the spirit of expediting the prosecution of the present application, applicant has clarified each of the independent claims as follows to further distinguish the prior art of record:

"detecting a plurality of malware events each with one of a plurality of levels using a malware scanner, the plurality of malware events comprising ~~at least one~~ ~~of~~ completion of a malware scan, a process failure relating to malware scanning, a missing log file, detection of malware, ~~or~~and failure of a response to malware."

Applicant respectfully asserts that simply nowhere in the references relied on by the Examiner is there any disclosure of malware events including "completion of a malware scan, a process failure relating to malware scanning, a missing log file, detection of malware, and failure of a response to malware," as presently claimed by applicant (emphasis added). A notice of allowance or a proper prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. Just by way of example, with respect to Claims 52-53 et al., the Examiner has relied on paragraphs [0027-0029] in Ackroyd to make a prior art showing of applicant's claimed techniques "wherein if the level of the detected malware event is less than the event trigger threshold, the notification of the event is not transmitted until an eventual periodic event transmission" (Claim 52 et al.) and "wherein if the level of the detected malware event is less than the event trigger threshold, the notification of the event is not transmitted until a request by a management server is received" (Claim 53 et al.). The Examiner has specifically argued that in Ackroyd "the system waits for predetermined regular times to occur at which the policy organizing server 32 issues queries to the database to generate the predetermined reports which are then compared with predetermined patterns and network-wide threshold to trigger predefined anti-malware actions."

Applicant respectfully asserts that, in Ackroyd, only the query for malware detections (i.e. malware that has already been detected) is made periodically, which clearly does not meet applicant's claimed "notification of the event [that] is not transmitted until an eventual periodic event transmission" and/or "until a request by a management server is received" (emphasis added).

Again, since at least the third element of the *prima facie* case of obviousness has not been met, a notice of allowance or a proper prior art showing of all of the claim limitations, in the context of the remaining elements, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

Additional Fees:

The Commissioner is hereby authorized to charge any insufficient fees or credit any overpayment associated with this application to Deposit Account No. 19-5127 (19903.0016).

Conclusion

In view of the foregoing, all of the Examiner's rejections to the claims are believed to be overcome. The Applicants respectfully request reconsideration and issuance of a Notice of Allowance for all the claims remaining in the application. Should the Examiner feel further communication would facilitate prosecution, he is urged to call the undersigned at the phone number provided below.

Respectfully Submitted,



Michael A. Schwartz
Reg. No. 40,161

Dated: January 24, 2006

Swidler Berlin, LLP
3000 K Street, N.W., Suite 300
Washington, D.C. 20007
(202) 424-7500